#2AO 106 (Rev. 06/09) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the
Eastern District of Missouri

IN THE MATTER OF THE SEARCH OF **One (1) Apple iPhone, in a black self-charging case, no identifiable exterior serial or model numbers; and One (1) Apple iPad Mini bearing serial number F9FWM0SBGEMHMN**	Case No. 4:20 MJ 6199 PLC *Signed and Submitted to the Court for filing by reliable electronic means* **FILED UNDER SEAL**

APPLICATION FOR A SEARCH WARRANT

I, Kent D. Layman, a federal law enforcement officer or an attorney for the government request a search warrant and state under penalty of perjury that I have reason to believe that on the following property:

One (1) Apple iPhone, in a black self-charging case, no identifiable exterior serial or model numbers; and One (1) Apple iPad Mini bearing serial number F9FWM0SBGEMHMN

located in the Eastern District of Missouri, there is now concealed

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ✓ evidence of a crime;
- contraband, fruits of crime, or other items illegally possessed;
- property designed for use, intended for use, or used in committing a crime;
- a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C., §§ 1028	Identity Theft

The application is based on these facts:

SEE ATTACHED AFFIDAVIT WHICH IS INCORPORATED HEREIN BY REFERENCE.

- ✓ Continued on the attached sheet.
- ❑ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

I state under penalty of perjury that the forgoing is true and correct

KENT D LAYMAN Digitally signed by KENT D LAYMAN Date: 2020.08.25 13:44:26 -05'00'

Kent D. Layman, Senior Special Agent USSS

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedures 4.1 and 41 on this 25th day of August, 2020

Date: August 25, 2020

Patricia L. Cohen
Judge's signature

City and State: St. Louis, MO

Honorable Patricia L. Cohen, U.S. Magistrate Judge
Printed name and title

AUSA: Jennifer J. Roy

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF MISSOURI

IN THE MATTER OF THE SEARCH OF **One (1) Apple iPhone, in a black self-charging case, no identifiable exterior serial or model numbers; and One (1) Apple iPad Mini bearing serial number F9FWM0SBGEMHMN**	)	Case No. 4:20 MJ 6199 PLC *Signed and Submitted to the Court for filing by reliable electronic means* **FILED UNDER SEAL**

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Kent D. Layman being duly sworn, depose and state as follows:

INTRODUCTION AND BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property, one electronic device, described in *Attachment A*, which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in *Attachment B*.

2. I am a Senior Special Agent with the United States Secret Service (hereinafter "USSS") and have so been employed since September 9, 2002. I am assigned to the St. Louis Field Office and am authorized to investigate criminal violations of federal law and to execute warrants issued under the authority of the United States. My specialized training includes successful completion and graduation from the Criminal Investigator Training Program of the Federal Law Enforcement Training Center and the United States Secret Service James J. Rowley Training Center. Through my training and experience, I have expertise in investigations involving counterfeiting, access device fraud, identity theft, financial institution fraud, wire fraud, mail fraud, and conspiracy to commit these acts.

3. The facts in this affidavit come from information obtained from information obtained from other law enforcement officers, and also includes information I obtained through my USSS training and experience. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all information collected during the course of this investigation.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that **STEVEN KOURVOISSEUR BRYANT** (hereinafter "**BRYANT**"), and other known and unknown persons, have committed identity theft, in violation of 18 U.S.C. §1028(a)(7) (hereinafter "Subject Offense"). There is also probable cause to search the electronic devices described in *Attachment A* for evidence of this crime and contraband or fruits of this crime, as described in *Attachment B*.

LOCATION TO BE SEARCHED AND IDENTIFICATION OF THE DEVICE

5. The property to be searched is:

(a) **One (1) Apple iPhone, in a black self-charging case, no identifiable exterior serial or model numbers; and**

(b) **One (1) Apple iPad Mini, bearing serial number F9FWM0SBGEMHMN**

(hereinafter referred to collectively as "**Devices**"). The **Devices** are currently located at the United States Secret Service, St. Louis Field Office, located at 111 S. 10th Street, Suite 11.346.

6. The applied-for warrant would authorize the forensic examination of the **Devices** described in *Attachment A* for the purpose of identifying electronically stored data particularly described in *Attachment B*.

TECHNICAL TERMS AND DEFINITIONS

7. Based on my training and experience, I know the terms described below have the following meanings or characteristics:

a. Wireless telephone: A wireless telephone (a/k/a "mobile" telephone or "cellular" telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. "Computer" means an electronic, magnetic, optical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device. *See* 18 U.S.C. § 1030(e)(1). Computers are physical units of equipment that perform information processing using a binary system to represent information. Computers include, but are not limited to, desktop and laptop computers, smartphones, tablets, smartwatches, and binary data processing units used in the operation of other products like automobiles.

c. "Computer hardware" means all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices

such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, modems, routers, scanners and related communications devices such as cables and connections), as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).

d. "IP Address" (a/k/a Internet Protocol address) is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

e. "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the internet, connections between devices on the internet often cross state and international borders, even when the devices communicating with each other are in the same state.

8. Based on my training and experience, and research, I know that the **Devices** have capabilities that allows them to serve as a wireless telephone, digital camera, portable media player, and GPS navigation device.

9. Therefore, in my training and experience, examining data stored on the **Devices** may uncover, among other things, evidence that reveals or suggests who possessed or used the **Devices** and how the **Devices** were used.

PROBABLE CAUSE

10. Your affiant is familiar with the facts in this investigation in the following way: I responded to the Florissant Police Department (hereinafter "FPD") at the request of Police Officer Jon Kemp (hereinafter "PO Kemp") and reviewed the evidence, including the **Devices**. I spoke with PO Kemp on several occasions regarding this case and reviewed videotaped interview of **BRYANT**.

11. On May 15, 2020, FPD Officer Kemp was on routine patrol when he observed a blue Audi Q5, with no vehicle license plate on the front of the vehicle. PO Kemp also noted that the Audi was equipped with vision reducing material covering the entire front windshield. Florissant Municipal Code 380.180, forbids front windshield window tinting beyond the manufacture tinting at the top of the front windshield. PO Kemp was able to observe the rear of the Audi as it passed his patrol car and observed that the Audi had a Tennessee temporary vehicle plate bearing GV34MP. PO Kemp conducted a computer inquiry and determined that the license plate showed no registration on file.

12. PO Kemp conducted a traffic stop of the Audi at North Waterford Drive, Florissant, Missouri. **BRYANT** was the driver and sole occupant of the vehicle. PO Kemp advised **BRYANT** why he had stopped his car. **BRYANT** provided PO Kemp with an Arkansas driver's license and stated that he did not have insurance. Based on the number and variety of violations, PO Kemp decided to conduct a further investigation and asked **BRYANT** for his consent to search his vehicle. **BRYANT** provided PO Kemp with his knowing and voluntary consent.

13. PO Kemp conducted a law enforcement database computer inquiry prior to searching the car and found that **BRYANT'S** driving status had been suspended. Further, the Audi's Vehicle Identification Number (hereinafter "VIN") showed no registration on file through Tennessee.

14. FPD Officer Matthew Luber (hereinafter "PO Luber") arrived on the scene to assist in the investigation. PO Kemp again asked **BRYANT** for consent to search his vehicle and **BRYANT** provided his consent for a second time.

15. PO Kemp conducted a search of the vehicle and recovered **Device (a)** from the center console and **Device (b)** in the driver side door pocket. PO Kemp also recovered from throughout the vehicle: eight (8) blank credit/debit cards; one (1) credit/debit device embossed with "Preferred Customer"; two (2) credit/debit cards bearing the name "Steven Bryant"; one (1) credit card reader; one (1) blank State Farm paper check; and eleven (11) credit/debit devices with microchip and bank logos.

16. PO Kemp advised that he asked **BRYANT** if he could search his person and that **BRYANT** provided his knowing and voluntary consent. PO Kemp recovered the following items from **BRYANT**: ten (10) credit/debit devices embossed with the name "Steven Bryant"; one (1) blank credit/debit device; and one (1) credit debit device embossed with "Temporary Card Only."

17. PO Kemp detained **BRYANT** by placing him in handcuffs. PO Kemp advised **BRYANT** of his constitutional rights pursuant to *Miranda v. Arizona*. **BRYANT** acknowledged that he understood his rights, waived his rights, and made a knowing and voluntary statement. **BRYANT** stated that he lost his wallet and was trying to obtain new cards. **BRYANT** had no explanation for cards that lacked account numbers or account holder names. **BRYANT** advised he bought the blank cards online.

18. At this time PO Kemp placed **BRYANT** under arrest for Driving while Operator's License was Suspended and Possession of a Forging Instrument.

19. On May 16, 2020, I responded to the FPD to review the evidence. I used a card reader connected to a USSS issued laptop to run cards seized during the course of this investigation. Approximately thirteen access devices were determined to be counterfeit or unauthorized in that the information embossed on the cards did not match the account information encoded on the magnetic strips.

20. On May 16, 2020, PO Kemp conducted a videotaped interview of **BRYANT** at the FPD. I have reviewed the video recording of this interview. PO Kemp again advised **BRYANT** of his constitutional rights pursuant to *Miranda v. Arizona* and **BRYANT** waived his rights and made a knowing and voluntary statement. **BRYANT** admitted to purchasing the re-encoding device, white plastic cards, and partially made credit cards online via the "dark web." **BRYANT** stated that some of the purchased cards were already encoded with other individual's credit card numbers. **BRYANT** stated had re-encoded one (1) personal credit card with one of his old account numbers because his wallet had been stolen. PO Kemp asked **BRYANT** if he would unlock the **Devices** and allow the officer to view the contents. **BRYANT** initially declined to give consent. PO Kemp advised **BRYANT** that he would obtain a search warrant for the **Devices** and continued the interview. **BRYANT** admitted that he used an application (hereinafter referred to as "app") called "Telegram" to receive stolen account information and personal identification information provided to him by other unidentified individuals. After further discussion about whether he would or would not provide consent to search the **Devices** as well as the possible course of the investigation, **BRYANT** stated, "Well, come on. Let's get it started."

21. **BRYANT** first entered his passcode into **Device (a)** and opened that device. **BRYANT** directed PO Kemp to the Telegram app he used to obtain bank account and personal information.

22. **BRYANT** advised that the same type of information, to wit, bank account and personal information obtained using the Telegram app, would be found on **Device (b),** entered his passcode, and opened **Device (b)**. **BRYANT** stated that the Telegram app was not loaded on that device but instead he used a VPN to access a web browser to go to a card site where stolen information on the site is stored. PO Kemp noticed a "Social Security Number Validator." **BRYANT** advised that he was "experimenting" with that. **BRYANT** stated that he connected the encoder to **Device (b)** via an app using Bluetooth.

23. Based on my training and experience and research, I know that "Telegram" is a cloud-based instant messaging and voice over IP service. I know that Telegram's privacy policy claims that all messages and stored data is encrypted.

24. Based on my training and experience, I know that individuals who are engaged in identity theft and credit card fraud, such as the criminal activity described above, use a variety of electronic devices as tools of the trade. Such subjects routinely use computers, tablets, and cellular devices to communicate with other members of the scheme, search for addresses of potential victim businesses, and search for and store stolen personal and bank account information. I know that stolen information is easily stored and transported from place to place and shared between devices. Further, the presence of items such as blank credit/debit cards and counterfeit cards in addition to the information located on the **Devices** that are the subject of this warrant, indicates that this scheme involved not only the possession of stolen personal identification information but most likely the actual theft of that data and production of counterfeit access devices.

25. In summary, I believe based on the facts outlined herein and my training and experience, that there is ample probable cause to conclude that **BRYANT**, likely being aided and abetted by others known and unknown, committed identity theft, in violation of 18 U.S.C. §1028(a)(7) and, further, that the **Devices** identified herein operated as instrumentalities of this crime. As outlined above, the investigation revealed that **BRYANT** is a resident of Arkansas with no verified ties to the Eastern District of Missouri. **BRYANT** was operating an unregistered vehicle with a counterfeit Tennessee temporary license plate. I know that individuals engaged in this manner of fraud frequently travel to other States for short periods of time to use fraudulent credit devices and move on prior to detection of the scheme by law enforcement. Here, **BRYANT'S** use of an unregistered vehicle with invalid plates is a further indication that he was attempting to conceal his identity and criminal conduct from law enforcement. PO Kemp recovered counterfeit access devices from **BRYANT'S** possession. **BRYANT** also made knowing and voluntary statements admitting to obtaining stolen personal identification information from the "dark web" and advised that he used an app to trade stolen information with other unidentified individuals. These statements and the recovered counterfeit access devices containing stolen bank account information clearly reflects there is probable cause to conclude that **BRYANT** did commit identity theft in violation of 18 U.S.C. §1028(a)(7). Because the **Devices** seized during the course of this investigation were being used to facilitate this scheme, I believe that the **Devices**, therefore, will likely contain evidence relevant to the known victims and may also identify additional victims of this scheme.

26. I note that although **BRYANT** arguably gave consent to the FPD to search the **Devices** during the May 16, 2020 custodial interview, and that the investigative agencies might already have all necessary authority to examine those items, I am requesting a warrant, out of an

abundance of caution, to be certain that an examination of the **Devices** will comply with the Fourth Amendment and other applicable laws.

27. The **Devices** are currently in the lawful possession of the USSS. The **Devices** were originally seized and stored by the FPD. The FPD did not search the **Devices** beyond the consensual review of the **Devices** during the May 16, 2020 custodial interview described above. In my training and experience, I know that upon delivery to the USSS, the **Devices** have been stored in a manner in which the contents are, to the extent material to this investigation, unaltered since the time when the **Devices** first came into the possession of the investigative agencies.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on **Device (b)**, the tablet, may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Digital information on a computer, mobile phone, tablet, or other similar electronic media can be saved or stored on the device intentionally, i.e., by saving an e-mail as a file, or saving the location of one's favorite websites such as "bookmarked" or "favorite" files. Digital information can also be retained unintentionally, such as traces of the path of an electronic communication that may be automatically stored in many places (e.g., temporary files or internet Service Provider client software, among others). Applications operating on electronic devices also store data about the device user, times and locations of when an application may be operated by the user, and other data related to the general use of the application (such as a photo, a message, a search, etc.)

c. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

d. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

e. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache.

30. *Forensic evidence*. As further described in *Attachment B*, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how each **Device** was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the **Devices** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. Nature of examination. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the **Devices** consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the **Devices** to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

32. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the **Devices** described in *Attachment A* to seek the items described in *Attachment B*.

33. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

34. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation into the criminal organizations as not all of the targets of this investigation will be searched at this time. Based upon my training and experience, I have learned that, online criminals actively search for criminal affidavits and search warrants via the internet, and disseminate them to other online criminals as they deem appropriate, *i.e.*, post them publicly online through the carding forums. Premature disclosure of the contents of this affidavit

and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

I state under penalty of perjury that the forgoing is true and correct

KENT D LAYMAN Digitally signed by KENT D LAYMAN Date: 2020.08.25 10:34:45 -05'00'

Kent D. Layman, Senior Special Agent
UNITED STATES SECRET SERVICE

Sworn to, attested to, and affirmed before me via reliable electronic means pursuant to Federal Rules of Criminal Procedure 4.1 and 41 this 25th day of August, 2020.

Patricia L. Cohen

The Honorable Patricia L. Cohen
United States Magistrate Judge

ATTACHMENT A
DESCRIPTION OF MEDIA TO BE SEARCHED

The property to be searched is:

(a) One (1) Apple iPhone, in a black self-charging case, no identifiable exterior serial or model numbers; and
(b) One (1) Apple iPad Mini, bearing serial number FWM0SBGEMHMN

(hereinafter collectively referred to as "**Devices**"). The **Devices** are currently located at the United States Secret Service, St. Louis Field Office Evidence Vault, located at 111 South 10th Street, Suite 11.346, St. Louis, MO, 63102.

This warrant authorizes the forensic examination of the **Devices** for the purpose of identifying the electronically stored information described in *Attachment B*.

ATTACHMENT B

1. All records on the **Devices** described in *Attachment A* that relate to violations of 18 U.S.C. §§1028(a)(7) (identity theft), (hereinafter the "Subject Offense") and involve **STEVEN KOURVOISSEUR BRYANT** (hereinafter "**BRYANT**") from January 1, 2019 to May 15, 2020, including:

a. Information relating to who used or communicated with the **Devices**, including records about their identities and whereabouts;

b. Communications or draft communications pertaining to, about, or mentioning the following: counterfeiting, access device fraud, identity theft, credit card fraud, counterfeit access devices, unauthorized access devices, device-making equipment, skimmers, and card encoding devices;

c. Preparatory steps taken in furtherance of a scheme and conspiracy to commit the Subject Offense including travel arrangements, receipts for purchase of tools and other equipment;

d. Financial records relating to the Subject Offense, including the use of bank accounts in connection with the movement and disposition of funds;

e. Information relating to who created, used, or communicated with the **Devices** described in *Attachment A*, including records about their identities and whereabouts;

f. Evidence indicating how and when the **Devices** described in *Attachment A* were accessed or used, to determine the geographic and chronological

context of access, use, and events relating to the crime under investigation and to the device owner;

g. Evidence indicating the device owner's state of mind as it relates to the crime under investigation;

h. The identity of the person(s) who used the **Devices** described in *Attachment A*, including records that help reveal the whereabouts of such person(s);

i. The identity of the person(s) who communicated with the user of the **Devices** described in *Attachment A* about matters relating to the scheme or conspiracy, including records that help reveal their whereabouts;

j. Identification of additional co-conspirators, accomplices, and aiders and abettors in the commission of the above offenses; and

k. All bank records, checks, credit card bills, account information, and other financial records.

2. Evidence of user attribution showing who used or owned the **Devices** at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

3. Records evidencing the use of the internet including:

a. records of Internet Protocol addresses used; and

b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

4. As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have

been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.